CERTIFICATE OF MAILING BY EXPRESS MAIL
"EXPRESS MAIL" Mailing Label No EL706391860US

Date of Deposit: October 22, 2001
I hereby certify that this paper or fee is being deposited with the U S Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1 10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Application, Washington, D C 20231

Type or Print Name Marcy Overstreet
Signature Marcy Overstreet

LOCATION PRIVACY PROXY

Applicant(s): Afshin Abtin
Olof Jansson

TECHNICAL FIELD

The present invention relates to mobile positioning on the mobile Internet, and more particularly, to protecting the privacy of mobile devices communicating with the mobile Internet.

BACKGROUND OF THE INVENTION

The mobile Internet, and especially location based services (LBS) are evolving applications relating to the use of the Internet. Additional terminal capabilities and the 3G service network are beginning to reach the market. The development of these services places at issue the privacy of end users and devices utilizing these services.

As the use of the mobile Internet expands, the resolution of security and privacy issues will become increasingly important. End users will desire to maintain the privacy and security of various types of data associated with devices with which they access the mobile Internet including things such as the MSISDN (phone number), location data associated with the mobile device, time and time related data, services accessed by an end user, and user IDs and passwords. Along with these expanded desires of end users to protect certain types of user information has come the development of laws relating to the mobile Internet and particularly location information associated with users. Countries are beginning to propose regulations on how the location of end users may be processed and provided to third parties.

While present mobile location applications are usually based upon a user initiated location request provided directly and only to the user, future applications such as network initiated positioning or triggers causing the position of an end user to be tracked, raise increased privacy aspects with respect to the party requesting positioning information. Thus, some manner for providing user control of location data and other types of privacy information would be greatly beneficial in the developing uses of the mobile Internet.

SUMMARY OF THE INVENTION

The present invention overcomes the foregoing and other problems with a system and method wherein upon receipt of a request to position a user using location based services (LBS), a location privacy proxy (LPP) is accessed to determine whether or not the LBS is allowed to position the user. Responsive to this determination, the user may then, or may not, be positioned.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be obtained by reference to the following Detailed Description when taken in conjunction with the accompanying Drawings wherein:

FIGURE 1 is a block diagram of an environment of operation of the location privacy proxy of the present invention; and

FIGURE 2 is a flow diagram illustrating the operation of the location privacy proxy;

FIGURE 3 is a flow diagram illustrating positioning with an untrusted application;

FIGURE 4 is a block diagram of an alternative environment of operation of the location privacy proxy of the present invention;

FIGURE 5 illustrates a first positioning scenario in the system of FIGURE 4; and

FIGURE 6 illustrates a second positioning scenario in the system of FIGURE 4.

DETAILED DESCRIPTION

Referring now to the drawings, and more particularly to FIGURE 1, there is illustrated a network 10 incorporating the location privacy proxy 15 of the present invention. The end user 45 comprises a user utilizing a mobile communication device such as mobile telephone, personal data assistant, pager, laptop computer or other type of mobile device which may wirelessly access the mobile Internet. The access server 50 provides access to a PLMN (not shown) using the WAP protocol by end user 45. The WAP gateway proxy 55 acts as an interconnect between the PLMN and an external network (i.e., the Internet 65) utilizing a protocol other than the WAP protocol such as an IP protocol. The mobile portal

25 provides an access point for the end user 45 to select particular services to be provided or not provided to the end user 45. The location privacy proxy 15 is located within secure equipment 20 having interfaces with the mobile portal 25, location based services (LBS) 30, gateway mobile positioning centers (GMPC) 35 and LDAP (Lightweight Directory Access Protocol) profile database 40. The LDAP profile databases 40 comprise server nodes serving as catalogues and/or subscriber databases and are normally controlled by an operator. The LPP 15 is a centralized privacy control function separated from the positioning systems. The LPP 15 uses end user profiles stored within the LDAP profile database 40 or responses received from an end user 45 through the access server 50, WAP gateway proxy 55 and the mobile portal 25 to determine if the user may be positioned. The LPP 15 provides a standardized interface between the LBS 30 and the positioning systems. The LPP 15 enables a user to manually override these privacy settings whenever there is a conflict between the privacy policy of the user and the privacy policy of the LBS 30. This allows positioning in special cases where privacy levels do not agree. The overrides must be confirmed by the user using SMS. The positioning systems include the gateway mobile positioning centers 35 and the serving mobile positioning centers (SMPC) 60.

The positioning information for an end user 45 is obtained from a PLMN network 65 through the GMPCs 35 and the SMPCs 60. User profiles associated with an end user 45 are stored within the LDAP profile database 40. The user profiles stored within the LDAP profile database 40 contain information describing the applications which may position the end user 45. This may be done by user established privacy preferences. One example of privacy preferences includes ranking applications with privacy level one, privacy level two

or privacy level three. Privacy level one is associated with trusted applications which are normally located within a system operator's domain and does not require accessing an external network such as the Internet. Privacy level two applications are semi-trusted applications which are offered by partners of the system operator. Finally, privacy level three applications are untrusted applications which are from unknown parties to which no particular trust level may necessarily be imparted. Additional privacy level definitions may include, but are not limited to, no positioning wherein the end users will not allow themselves to be positioned at all, and a black listing wherein end users may define specific applications to not be able to position a user despite the established privacy level of the end user and the application. The privacy level of an application is set by the network operator based on similar criteria, and stored in the LDAP profile database 40 as one of the services available to end users 45.

Referring now to FIGURE 2, there is a flow diagram illustrating a use case of the LPP 15 of the present invention. The mobile portal 25 offers a number of LBS 30 which may be selected by either the end user 45 or a third party interacting with the mobile portal 25 via a network 65, such as the Internet. One of the LBS is selected at step 80 and the portal 25 asks the location privacy proxy 15 at step 85 for privacy control of the requested location based service. The LPP 15 determines at inquiry step 90 whether this is the first time the user is requesting this particular LBS 30. If so, the LPP 15 determines at inquiry step 100 whether the end user 45 has authorized use of the LBS 30 by accessing the user profile within the LDAP profile data base 40 or asking the end user 45 directly through the mobile portal 25. If the use of the LBS 30 is authorized, the application is added to the user's list of

allowed applications within the LDAP profile database 40 at step 110. If the service 30 is not authorized, inquiry step 102 determines if the user manually overrides to enable positioning. If inquiry step 90 determines that this is not the first time for the end user 45 to access the location based service 30, the LPP 15 will assess the LDAP profile database at step 93, inform the portal at step 95 of the user's privacy preferences for the request, and determine whether the location based service is authorized at step 100.

If the LBS 30 is authorized to position the end user 45, the LPP 15 will obtain the position of the end user from the GMPC 35 and attach this information to the position request at step 125. It is up to the operator to define whether the MSISDN of the end user is sent to the LBS 30 based upon whether the application is a trusted or untrusted entity.

Referring now to FIGURE 3, if the LBS 30 is not a trusted application, the LPP 15 may be configured to act as a broker between the untrusted application and the GMPC 35. The GMPC 35 (Gateway Mobile Positioning Center) is a proprietary term for GMLC (Gateway Mobile Location Center) which is in the GSM standard. The GMPC 35 collects the position coordinates for a device connected to a certain MSISDN. The LPP 15 opens a session database at 115 responsive to the incoming request from the portal 25. The LPP 15 generates and attaches at step 120 a unique ID for the request before transmitting this information to the LBS 30. The unique ID will be mapped internally to the MSISDN of the end user 45 making a request by the LPP 15. The LPP will not keep the MSISDN and the position data together. This means that internal privacy issues will be secured by not relating the MSISDN with the end user 45 position information. The LBS 30 will ask the LPP 15 for

the positioning request at step 130 and the LPP 15 will communicate at step 135 the positioning request to the GMPC 35.

The end user 45 may also ask the portal 25 to always use the LPP 15 with any location related request. The LPP 15 will also offer an interface toward an SMS-C gateway (not shown) which will enable untrusted applications to send out SMS messages. These applications will not have access to the MSISDN numbers, only a unique ID generated by the LPP 15. Additionally, the LPP 15 may offer other interfaces such as multimedia messaging server (MMS) to enable untrusted applications to communicate with the end users through the LPP.

Referring now to FIGURE 4, there is illustrated an alternative embodiment wherein the location privacy proxy 15 is connected directly to a WAP gateway 55 without utilizing a portal connection as described in FIGURE 1. Other than the location privacy proxy 15 being directly connected to a WAP gateway 55, the configuration of the system 10 described in FIGURE 3 is identical.

Referring now also to FIGURE 5, there is illustrated a first scenario of operations via the system 10 described in FIGURE 4 wherein the GMPC 35 issues a positioning request at step 140. The request is routed at step 145 to the location privacy proxy 15. The request at the GMPC 35 may be initiated by an end user 45 directly accessing the GMPC 35 or by, for example, a fleet management application or a friend finder application trying to position a user. In either case, a GMPC 35 has access to the MSISDN of the user which is to be positioned. The GMPC 35 request is routed via the location privacy proxy 15 to achieve a higher privacy control, and enable a check of the privacy settings at step 150 by accessing the

LDAP profile/database 40 and checking the privacy settings associated with the MSISDN. Based upon the settings a positioning may either be performed or denied at step 155.

In an additional scenario illustrated in FIGURE 6, a user 45 generates a request at step 160, and the request is routed by the WAP gateway 55 to the location privacy proxy 15 at step 165. The LPP will check the user's privacy setting at step 170 by accessing the LDAP 40 and positioning is performed based upon the settings at step 175.

The previous description is of a preferred embodiment for implementing the invention, and the scope of the invention should not necessarily be limited by this description. The scope of the present invention is instead defined by the following claims.